УДК 343.2/7

ФИШИНГ: ПОНЯТИЕ, МЕХАНИЗМ, МЕРЫ ПРЕДУПРЕЖДЕНИЯ

Д. С. Захаров
курсант 2 курса факультета милиции
Могилевского института МВД
Научный руководитель: ***Д. И. Шнейдерова****,*
преподаватель кафедры уголовного процесса
и криминалистики Могилевского института МВД

Развитие высоких технологий и растущая популярность интернет-пространства обуславливают прогрессивность киберпреступности. Непрерывно совершенствующиеся навыки киберзлоумышленников ставят перед правоохранительными органами первостепенную задачу по разработке комплекса мер противодействия и профилактики новых видов таких преступлений, совершаемых в сети Интернет.

Одним из самых распространенных киберпреступлений 2019 — начала 2020 года является фишинг, под которым понимается интернет-мошенничество, совершаемое путем обмана пользователей с целью завладения их конфиденциальными данными (логины, пароли, приватные ключи и др.). Последующее использование указанных данных позволяет получить доступ к интернет-банкингу и электронным кошелькам, в том числе криптовалютным, с целью их хищения. В основе алгоритма фишинга лежит массовая интернет-рассылка писем из различных источников, информационная составляющая которых побуждает доверчивого пользователя следовать указаниям и совершать необходимые мошеннику действия. Такими действиями могут быть: ввод логина или пароля на подставном сайте, внешне схожим с оригинальным, либо сообщение в социальной сети от имени знакомого пользователю человека с просьбой о помощи, требующей сообщения конфиденциальных данных. По статистике, кибермошенник, разославший 10 писем-ловушек, имеет вероятность в 90 %, что как минимум 1 пользователь в нее попадется [1].

Представляется целесообразным проведение правоохранительными органами информирования пользователей как в сети Интернет, так и посредством личных бесед о соблюдении мер предосторожности, которые не позволят им стать «жертвами» фишинг-мошенников. Так, при получении подозрительного письма от администрации хорошо знакомого сайта целесообразно убедиться в правильном написании как доменного имени сайта, так и самого отправителя, так как чаще всего они отличаются лишь на 1–2 буквы (символа). Следует вни-

мательно ознакомиться и с содержанием письма. В большинстве случаев злоумышленники требуют активных действий от пользователя под угрозой ограничения его прав по использованию конкретного ресурса, что никогда не будут делать представители реальной администрации. Если дело касается взаимоотношений между знакомыми людьми, то лучше лишний раз убедиться в необходимости оказания человеку помощи посредством телефонной связи или личной встречи.

1. Безмалый В. Типы фишинговых атак и способы их выявления [Электронный ресурс] // Интернет-портал журнала «Открытые системы». URL: https://www.osp.ru/winitpro/2019/03/13054903/ (дата обращения: 28.01.2020). Вернуться к статье